ボットネットに見る日中両国のインターネット事情

楊　剣　　倪　永茂

1．はじめに

電子政府・電子商取引等社会のIT化に伴い、インターネットは社会のインフラとなりつつある。同時に、社会のIT化から派生する様々な問題、とりわけ、ネットワーク不正アクセスやサイバー犯罪等も顕在化してきた。本文では、近年出現した新たなインターネット攻撃の土台であるボットネットを取り上げ、日中両国のインターネット事情を比較分析する。

利用する基礎データとして、中国ネットワークインフォメーションセンター（CNNIC）の発表した「全国ネットワーク安全状況調査報告」および「工作報告」、日本警察庁セキュリティポータルサイト（@Police）の公表データを利用する。両サイトはそれぞれの国における権威ある機関であるからである。

本文でいう「ボット（bot）」とは、知らないうちに悪意のある人物に乗っ取られたコンピュータのことを指す。こうした状態に置かれたコンピュータのことを「ゾンビ」と呼ぶ場合もある。また、こうした状態に置かれたコンピュータによって構成されたネットワークを「ボットネット（botnet）」と呼ぶ。ボットネットに組み込まれるコンピュータの数は世界規模で数百万台に上るとも言われている（警察庁@police（2005））。

ボットにされてしまったコンピュータは、外部から操作できるようになっているが、ふだん、コンピュータの挙動に見た目は変化なく、コンピュータの所有者、あるいは利用者に気づかれない。しかし、悪意に満ちた外部の人物から指令を受けると、迷惑メールを一斉送信したり、特定のサイトへ攻撃したり、様々なサイバー犯罪を起こすので、ボットネットの存在はインターネットにとって大きな脅威となっている（高橋正和（2006））。

近年、中国ではIT化が急進展している。CNNICの発表によると、2000年から2006年６月末までの間に、インターネットの利用者数では2000年の2,250万人から2006年６月末の1.23億人へと急増、インターネット接続可能なコンピュータ台数も2000年の892万台から2006年６月末の5,450万台にまで増えてきた。ISPの国際専用回線の容量も、2000年の2,799Mbpsから2006年６月末の214,175Mbpsに大きく増強された。一方、日本総務省によると、2005年日本のインターネット利用者数は8,529万人であった。規模から見ると、中国は既

日時	利用者数(万人)	前年度比
1998年06月末	117.5	－
1998年12月末	210	－
1999年06月末	400	240.4%
1999年12月末	890	323.8%
2000年06月末	1,690	322.5%
2000年12月末	2,250	152.8%
2001年06月末	2,650	56.8%
2001年12月末	3,370	49.8%
2002年06月末	4,580	72.8%
2002年12月末	5,910	75.4%
2003年06月末	6,800	48.5%
2003年12月末	7,950	34.5%
2004年06月末	8,700	27.9%
2004年12月末	9,400	18.2%
2005年06月末	10,300	18.4%
2005年12月末	11,100	18.1%
2006年06月末	12,300	19.4%
2006年12月末	13,700	23.4%

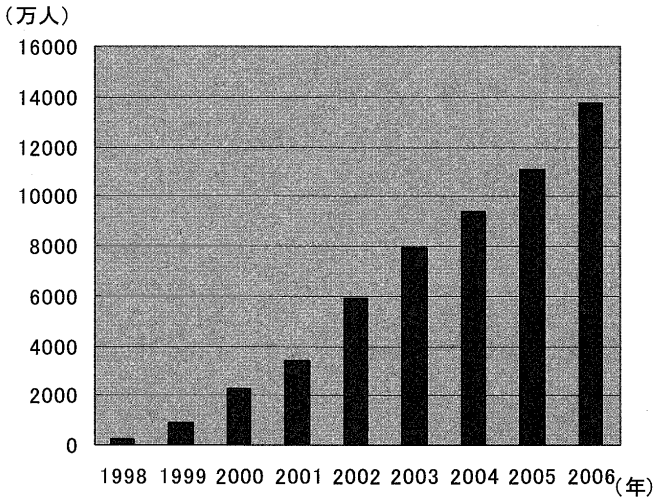

図１　中国インターネット利用者の推移（CNNICの発表による）

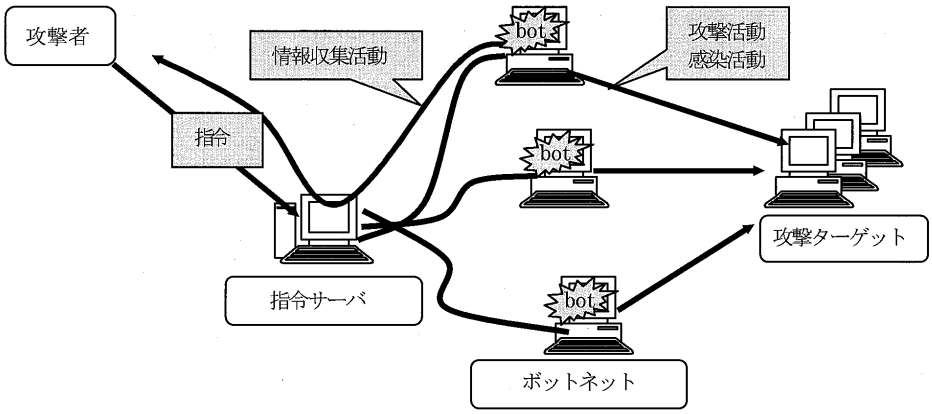

図２　ボットネットの構成と活動イメージ

に日本に匹敵するIT大国となっているといえよう。

中国でのインターネット使用者数の推移を図１に示す。

２．ボットネットの仕組み

ボットネットを利用したインターネット攻撃は近年出現したものである（高橋正和（2006））。

ボットとなったコンピュータは、コンピュータウィルスや、プログラムの脆弱性が悪用される等して、遠隔で操作できる状態にされてしまい、ひたすら外部からの指令を待つ。ボットネットは、指令を出す攻撃者、指令を送信するサーバ、ボットによる構成されたコンピュータ・ネットワークからなる（図２）。指令の通信にIRCプロトコルが使われることが多いが、一部HTTPプロトコルを利用するものもある（久米原栄（2001）、白井雄一郎他（2001）、Joel　Scambray他（2001））

攻撃者がDoS攻撃[1]の命令を指令サーバ経由で送信すると、各ボットは一斉に指定されたサイトに対してDoS攻撃を行う。ボットの数は数千台から数百万台まで非常に多いので、ターゲットにされたサイトがサービス不能に落ち、深刻な被害を被ることになる。

DoS攻撃のほかに、他のコンピュータへの感染活動、迷惑メールの送信、特定の広告サイトのアクセス、情報収集等、参加するコンピュータの数が多ければ効果が望まれる活動に悪用されてしまう。

インターネットにとってボットネットが大きな脅威である理由は以下のようにまとめられる。①世界規模のボットネットに対する防御手段は限られており、深刻な被害をもたらす危険性が高いこと、②雛形となるソースコードがインターネット上で流通していて、毎日約80種類のボット用プログラムの亜種が発生しているため、アンチウイルスソフトのシグネチャによる対応に限界があること、③攻撃者は指令サーバを通してボットネットを制御するため、攻撃者を特定することが困難であること、④いたずら目的ではなく金銭狙いのプロフェッショナルが関与するようになり、ボットネットを売買するブラックマーケットが存在していることが脅威を増長させている。

日本では、ボットネットの悪用に対する検挙事例はまだないが、中国ではボットネットによるネットワーク不正アクセス事件が数多く存在する。

2004年中国CNCERT／CCが処理した分散式DoS（DDoS）攻撃事件においては、被害側が長時間かつ継続的なDDoS攻撃を受け、攻撃パケットのデータトラフィックは1000Mも超え、攻撃手法は11種類に上り、被害側の営業は完全に停止させられ、相当な経済損失を出してしまった。調査結果によると、DdoS攻撃は大規模なボットネットを通じて行われていた。その目的は、被害側サイトの業務を停止させることによって競争の優位に

1　Denial of Service Attack。サービス妨害攻撃またはサービス不能攻撃などと呼ばれ、インターネット経由での不正アクセスの１つ。大量のデータや不正パケットを送りつけるなどの不正な攻撃を指す。

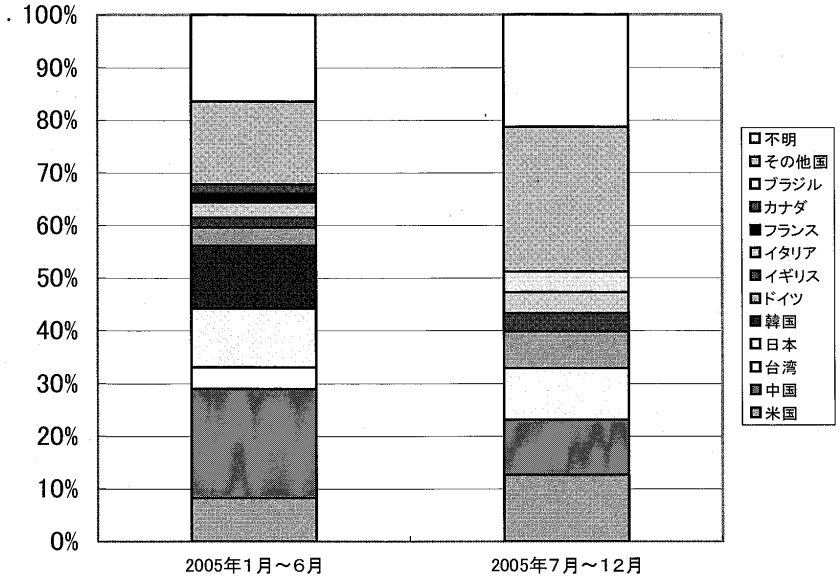

図３　ボットの国地域別台数

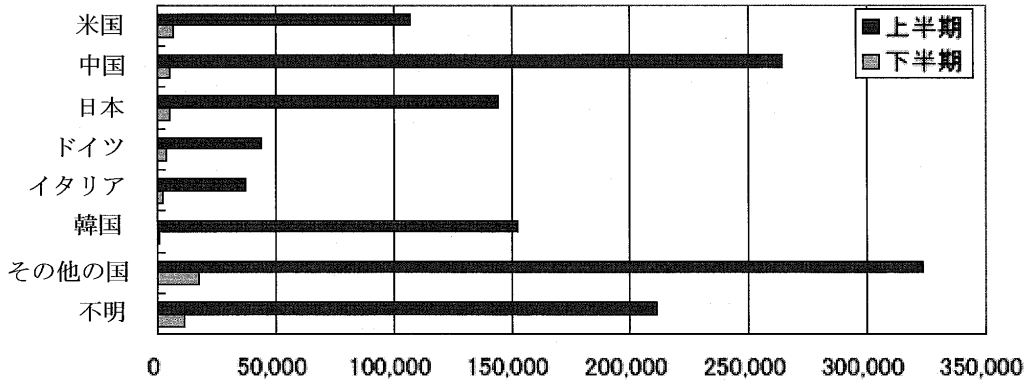

図４　ボットの国地域別比率（2005 年）

立つことであった。

また米国では、DoS攻撃等のためにボットネットを貸し出し、利益を得る等していた男に懲役４年９月の判決が出た事例がある。英国では、商用の賭博サイト対し「DoS攻撃を行う」として金銭を要求するサイバー恐喝が行われた。そういうことから、ボットネットを利用したインターネット攻撃は懸念され、とくに、サイバー兵器として懸念されている。日本@Policeは、今後特に警戒が必要と思われるものにボットネットを挙げている。また、ボットネットの現状を把握するために、2005年１月から観測システムを構築して運用始めている。

３．日中両国におけるボットネットの現状

ここでは、日中両国がそれぞれ発表したデータから、ボットネットに関する特徴を抽出し、比較分析を行う。

（１）中国と日本にあるボットが多い

日本@Policeが発表したデータによると、2005年以来、中国大陸内に属するIPアドレスのコンピュータの中にボット数は非常に多い。2005年１～６月の観測期間では、ボットと推定されたコンピュータのIPアドレスは世界では1,285,247存在しているが、約20.6％は中国大陸内に属するIPアドレスである。2005年７～12月の観測期間では、ボットと推定されるIPアドレス数は世界では52,732存在し、中国大陸内に属するIPアドレスと推定されるものは約10.4％を占めていた。

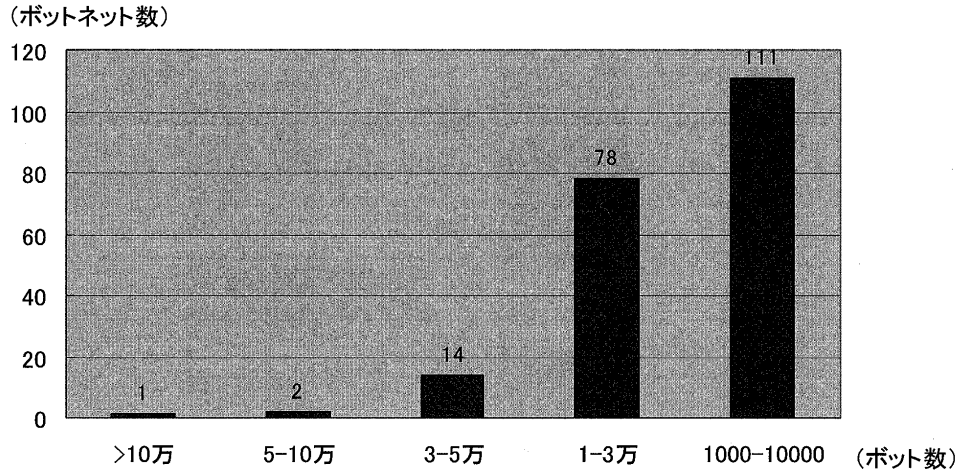

図5　2005年に観測されたボット数が1000以上のボットネット数（CNCERT/CCより作成）

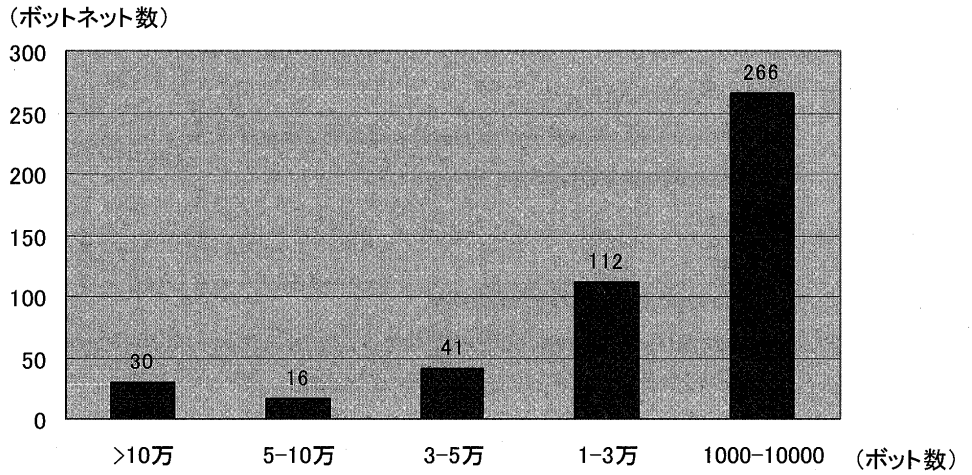

図6　2006年に観測されたボット数が1000以上のボットネット数（CNCERT/CCより作成）

一方、日本に属するIPアドレスと推定されるボット数、2005年１～６月の観測期間では全体の約11.2％を占めており、2005年７～12月の観測期間では全体の9.8％を占めていた。また、観測結果に記録されているドメイン名から、そのほとんどが個人ユーザと推測されると報告している。

とくに、2005年上半期においては、ボット数は主に日本を含む中国、韓国、香港、台湾等の東アジアの国・地域に多く、全体の５割近くを占めている（図３～４）。

（２）ボットの隠蔽工作が行われている

また、日本@Policeのボット観測データの下半期と上半期を比較すると、下半期のボット台数が上半期と比べて1,232,524台減、95.9％減で大幅に減少した。中国大陸に属するボット台数が上半期と比べ259,277台減、97.9％減で激減している。日本にあるボット台数も上半期と比べて139,334台減、96.4％減で大幅に減少している。一方、図４の「不明」となった発信元の国別が判別できないまたは意図的に隠されているIPアドレスの合計は全体に対する比率が、上半期の16.4％から下半期の21.3％に増加した。

その原因は以下のように考えられる。①最近ではボットネットの観測システムが存在することが広く知られており、意図的にIPアドレスを隠すようにボットが修正されたことが多くなってきていること、②個々のボットネットの規模が小さく

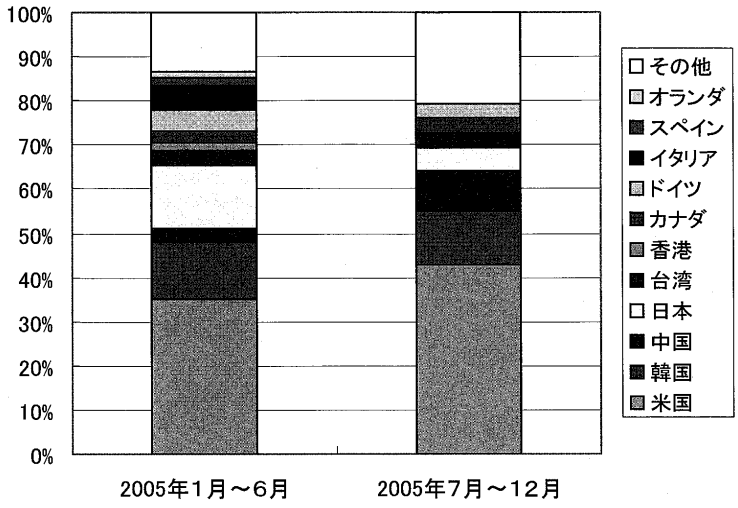

図7　指令サーバの国地域別比率（@Policeより作成）

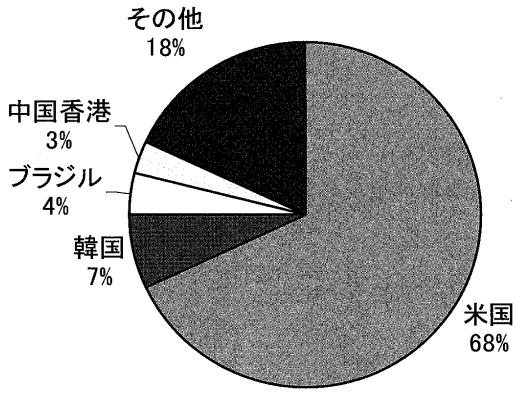

図8　2006年1～6月中国で観測した指令サーバの国地域別比率（CNCERT/CCより作成）

なっていること、③ボットネットがP２P（Peer to Peer）プロトコルやrootkit[2]を利用してその隠蔽性が高められたことである。

①については、日本@Policeによると、観測システムではボット数調査指令を指令サーバへ送信して、その結果をボット数として集計している。「下半期の減少は、ボット数調査指令に結果を返さないよう改造または設定変更された指令サーバが増加していると推測される。」と説明されている。

②に関しては、中国のCNCERT／CCの発表によると、2005年にはボット数が1000～10000規模のボットネットが111個観測され、全体の53.9%を占めている（図５）。2006年１～６月にはボット数が1000～5000規模のボットネットが266個観測され、全体の57.2%を占めている（図６）。このようにボットネットの規模に縮小する傾向が見られ、結果的にボットネット全体に接続するボット数が減少した結果をもたらした可能性がある。

③については、CNCERT／CCによると、2005年、P２Pプロトコルとrootkitを利用するボットが発見された。P２Pプロトコルの匿名性とrootkitの

2　コンピュータシステムへのアクセスを確保したあとで第三者（通常は侵入者）によって使用されるソフトウェアツールのセットである。こうしたツールは隠蔽する狙いがあり、ユーザに察知させることなく侵入者がシステムへのアクセスを確保できる。

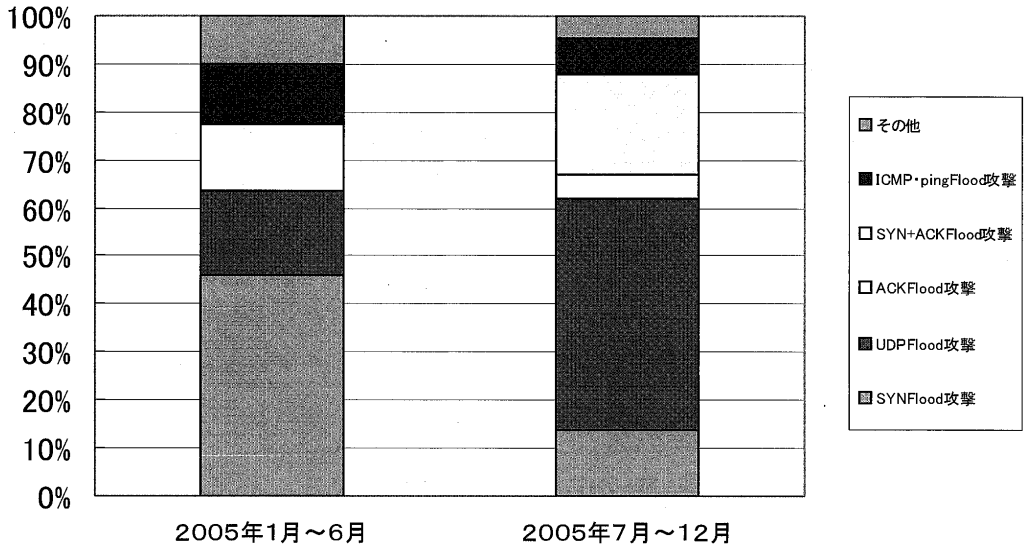

図９　攻撃活動命令手段別比率（@Police より作成）

隠蔽性が悪用されたと推測できる。

また、Telecom－ISACの小山覚氏によると、2004年にはSniffer[3]などを用いて指令サーバからボットに送られてくる指令の中身を把握することができたが、現在ではその内容が暗号化・略号化され、ボットネットが見えにくい存在になっている。このため、今後ボットネットの調査はより困難になると懸念されている。

一方、日本@Policeは2006年１～６月で観測したボットネット数は327で、2005年７～12月の196個に比べ約67%増加した。その中で新たに把握したものが234個あり、前期から継続して存在しているものが93個、今期に観測できなくなったものが103個ある。中国CNCERT／CCの2006年１～６月の観測期間ではボット数1000以上のボットネットが465個確認した、2005年の206個より約125.7%増加した。そのことから、ボットネットの規模が小さくなる一方、ボットネットの数が実質増加していると言えよう。

（３）指令サーバが多く米国にある

2005年日本@Policeの年間観測された指令サーバIPアドレス数は1,568あるが、IPアドレスが多い国は米国であり、全体の39.5%を占めた。日本のIPアドレスを使用している指令サーバの数も141とかなり多く、そのうちの126アドレスがDNS逆引きすると、国内プロバイダーのADSL等でよく使用される形式(IPアドレス＋ADSL等の文字＋ドメイン名）のホスト名であったことから、概ね個人ユーザのコンピュータと推測される。

図７は日本@Policeが観測している指令サーバの国地域別比率である。前期、後期を比べると上位にある米国と韓国の順位は変化していない。米国では前期の35.2%から後期の42.7%に増え、韓国では、前期の13.0%から後期の12.3%に横ばい状況である。日本では、前期の14.0%から後期の5.3%に減少した。中国では、前期の3.2%から後期の8.8%に増加した。

また、CNCERT／CCは2006年１～６月累計で約７百万IPアドレスが中国にあり、そのコンピュータがボットとなったと観測した。その指令サーバはやはり米国にあることが多い（図８）。

（４）攻撃ターゲットが多く米国にある

図９は@Policeが観測した攻撃活動命令の手段別比率を示す。その中、SYN　flood[4]攻撃が最も

3　ネットワーク上のパケットを傍受する行為を支援するソフトウェア。

4　インターネットにおけるDoS攻撃のひとつ。インターネット上に公開されているWWWサーバなどの負荷を増大させ、対象となるサイトを一時的に利用不能に陥らせてしまう効果がある。

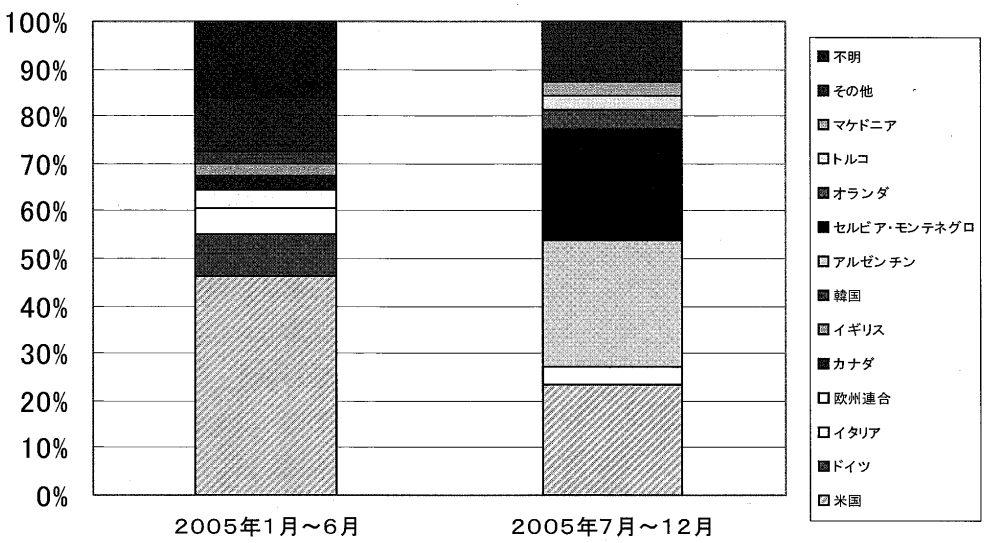

図10　攻撃先の国地域別比率（CNCERT/CCより作成）

多く、UDP flood[5]、ping flood[6] 等一般的に行われているDoS攻撃がほとんどである。その他として、TCPパケットをランダムに出す攻撃やボット毎の個別攻撃と推測されるもの等も観測されていると報道されている。

日本@Policeの2005年７～12月で観測したSYN flood攻撃は2005年１～６月と比べ81.5%減少したが、UDP flood攻撃は66.8%増加した。また、SYN flood・ACK floodを複合した攻撃が414.2%増加したことから、攻撃手法がより防御が困難なものに移行して行くことが推測できる。

SYN flood攻撃活動命令の宛先ポートは80／TCPが多い、WWWサービスを狙った攻撃により、WWWページを閲覧困難又は不能にさせることが目的と思われる。

一方、図10に示した通り、DoS攻撃を受けた国では米国が最も多く、2005年１～６月期間では被害全体の５割を占め、2005年７～12月期間では23.2%を占めていた。

日本への攻撃においては、2005年１～６月期間では攻撃先が特定できるものの3,531件中、７件とかなり少ないが、2005年７～12月期間では観測されなかった。

中国においては、2005年CNCERT／CCにインシデント届出を出した被害は11件があったことと、日本@Policeの観測データ中判明できたものの国別中中国は項目として例示していなかったことから、中国への攻撃が少ないと思われる。ただし、実際に攻撃があったが判明できなかった可能性も排除できない。

４．終わりに

本文は日中両国に公式に発表されたインターネットに関するデータから、ボットネットの現状について比較分析した。結論としては、①中国では日本よりもボット数が多いこと、②時間とともにボットの隠蔽工作も盛んに行われていること、③指令サーバも攻撃ターゲットも米国にあること、等が得られた。

さて、中国にボット数やボットネット数が多い理由は以下のように分析する。

①ブロードバンドの普及やインターネット常時接続環境の整備が進んだこと。

中国ではインターネット利用者数が日本を上回ったと同時に、ケーブルテレビに代表されたブロードバンドやインターネット常時接続の環境整備が大都市を中心にかなり進んできた。便利に

5　インターネットにおけるDoS攻撃のひとつ。コネクションレス型のUDPの特徴を利用し，連続したUDPパケットやサイズの大きいUDPパケットを送りつける攻撃。

6　pingコマンドにより膨大な数のICMP Echo Request パケットを送信する攻撃方法。

なった反面、コンピュータが外部からボットに感染され、本人の知らないうちにボットネットに組み込まれた危険性が飛躍的に高まった。

②オンライン利用が定着したこと

近年、コンピュータはワープロ等のオフライン利用から、WWW閲覧を中心としたオンライン利用に変わった。というよりも、むしろ、オンライン利用が一般的になってきた。とくに、中国ではQQに代表されるチャットや、日本よりも遥かに深刻な社会問題になりつつあるオンラインゲームを利用する人口が数千万にも上っている（CNNICの発表による）。つまり、同一ソフトが広範囲に利用されている特徴をもつ。そのソフトの脆弱性を利用したボットプログラムによって、たちまち大きなボットネットができてしまう。

③海賊版ソフトが氾濫していること。

中国では、８割のコンピュータに正規購入版ではなく、海賊版（コピー）ソフトが利用されているという（CNNICの発表による）。海賊版OSやソフトを不正に利用すると、その後のアップデートもできないことが多く、ボット用プログラムにとって絶好の感染ターゲットになってしまう。

従来のワームやウイルスといった脅威は、無差別な目標に対する脅威であり、また、深刻な脅威にいたるほどに広がるまでに、一定の時間を必要とした。これに対し、ボットネットを使った攻撃は、特定の相手を選択的に攻撃することが可能であり、また、瞬時に攻撃を開始することが可能である。さらに、ソースコードがインターネット上で流通しており、日々改良が加えられており、今後どのような方向に進んでいくのかは予断を許さない。

このようなボットネットの脅威に対応していくためには、正規版ソフトの使用や、ソフトのアップデート、セキュリティ意識を高める等の対策がコンピュータ利用者ひとりひとりに求められる。

無論、国もマスコミも、コンピュータ利用者に現在抱えている脅威がどのようなものであり、どのような対策が必要であるのかを、効果的に伝えていくことも必要であろう。

参考文献

高橋正和（2006）、「ITセキュリティの新たな脅威：ボットネット」『日本セキュリティ・マネジメント学会誌』Vol. 19、No. 2、pp.78－85

高橋正和他（2006）、「フィールド調査によるボットネットの挙動解析」『情報処理学会論文誌』Vol. 47、No. 8、pp.2512－2523

朝長秀誠他（2006）、「Botnetの命令サーバドメインネームを用いたBot感染検出方法」『情報処理学会研究報告』Vol. 2006、No.129、pp.13－18

久米原栄（2001）、『TCP／IPセキュリティ』ソフトバンク

白井雄一郎他（2001）、『不正アクセスの手法と防御』ソフトバンク

Joel Scambray他（2001）、『クラッキング防衛大全』翔泳社

CNCERT／CC（2003～2006）、「工作报告」

CNCERT／CC（2004）、「全国网络安全状况调查报告」

警察庁@police（2005）、「分析レポート：ボットネット（botnet）に注意」

通过 botnet 僵尸网络问题比较中日两国互联网

楊 剣　　倪 永茂

概　要

Botnet 被称作僵尸网络，是几千台乃至几百万台被恶意代码感染、控制的与互联网相连接的计算机网络系统。

本文通过分析比较中日两国有关 botnet 僵尸网问题的资料，得出了 3 个结论，即中日两国都存在很多 bot 僵尸及网络 它的隐蔽工作做的越来越好 它的控制者及入侵目标大多在美国。

随着互联网的迅速发展，给越来越多的普通用户带来便利的同时，也同时带来了风险。我们要采取安全配套措施，提高安全防备意识，使用正版软件，加强教育培训，让互联网更健康地发展。

(2007年 6 月 1 日受理)